

Kim D. Stephens
kstephens@tousley.com
Jason T. Dennett
jdennett@tousley.com
Tousley Brain Stephens PLLC
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992

Interim Lead Plaintiffs' Counsel

Keith S. Dubanevich
kdubanevich@stollberne.com
Yoon Park
ypark@stollberne.com
Stoll Berne
209 SW Oak Street, Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840

Interim Liaison Plaintiffs' Counsel

[Additional counsel appear on the signature page.]

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON**

IN RE: PREMIER BLUE CROSS
CUSTOMER DATA SECURITY BREACH
LITIGATION

This Document Relates to All Actions.

Case No. 3:15-md-2633-SI

**UNOPPOSED MOTION AND
SUPPORTING MEMORANDUM FOR
PRELIMINARY APPROVAL OF
PROPOSED SETTLEMENT
AGREEMENT**

LR 7-1 CERTIFICATION

In compliance with Local Rule 7-1(a), the parties, through their respective counsel, have conferred in multi-day mediation and settlement discussions between October 2018 and March 2019. Defendant Premera Blue Cross (“Defendant” or “Premera”) does not oppose this Motion.

MOTION

NOW INTO COURT, through undersigned counsel, come Plaintiffs Elizabeth Black, Catherine Bushman, Krishnendu Chakraborty, Maduhchanda Chakraborty, Ralph Christopherson, Anne Emerson, William Fitch, Eric Forsetter, Mary Fuerst, Debbie Hansen-Bosse, Stuart Hirsch, Ilene Hirsh, Howard Kaplowitz, Barbara Lynch, and Kevin Smith (“Plaintiffs”), individually and on behalf of the proposed Class, who hereby move this Court as follows:

1.

Plaintiffs’ Counsel, on behalf of Plaintiffs and the proposed Settlement Class, and Defendant have agreed on a proposed compromise settlement (the proposed “Settlement”) of all claims of the Class against Defendant, as more particularly set forth in and attached as Exhibit 1 (the proposed “Settlement Agreement” or “SA”), the terms, definitions, provisions, reservations and conditions of which are made part of this Motion.

2.

The purpose and intent of all parties to this proposed Settlement (the “Parties”) are: (a) to settle any and all claims of any type related to the cyberattack against Premera’s computer systems that was publicly disclosed on March 17, 2015 (the “Data Breach”); (b) to terminate and extinguish any liability of Defendant for all Released Claims of the Class Members; and (c) to dismiss on the merits and with prejudice all claims of the Class Members against Defendant.

3.

The Parties now seek preliminary approval from this Court of the terms of the proposed Settlement Agreement, including:

(1) Preliminary approval of the proposed Settlement memorialized in the proposed Settlement Agreement as being fair, adequate, and reasonable, such that notice to the Class should be provided pursuant to the proposed Settlement Agreement;

(2) Certification of the Settlement Class as defined in the proposed Settlement Agreement for settlement purposes only;

(3) Approval of a date for a Final Fairness Hearing;

(4) Approval of: (i) the Summary Notice to be mailed and/or emailed to proposed Settlement Class Members in a form substantially similar to the one attached to the proposed Settlement Agreement as Exhibit B; (ii) the Long Form Notice in a form substantially similar to the one attached to the proposed Settlement Agreement as Exhibit C; and (iii) the Publication Notice in a form substantially similar to the one attached to the proposed Settlement Agreement as Exhibit D;

(5) Approval of a Claims Deadline by which the Settlement Class Members shall be able to submit valid and completed Claim Forms;

(6) Appointment of Cameron Azari as the Notice Specialist as jointly agreed to by the Settling Parties;

(7) Appointment of Epiq as the Settlement Administrator as jointly agreed to by the Settling Parties;

(8) Setting a specified date by which objections shall be heard and papers in support of such objections must be submitted to the Court;

(9) Setting specified dates by which proposed Class Counsel shall file and serve all papers in support of the application for final approval of the proposed Settlement and by which the Parties shall file and serve all papers in response to any valid and timely objections and by which proposed Class Counsel shall file their motion for fees and expenses;

(10) Ordering that all proposed Settlement Class members will be bound by the Final Approval Order and Judgment;

(11) Ordering that persons in the Settlement Class wishing to exclude themselves from the proposed Settlement will have until the date specified in the Preliminary Approval Order to submit to the Settlement Administrator a valid written request for exclusion or opt out;

(12) Approving the proposed Settlement Agreement's procedure for persons in the proposed Settlement Class to object, including the right to object to Plaintiffs' attorneys' fees and costs, or opt out from the proposed Settlement;

(13) Approving deadlines consistent with the proposed Settlement Agreement for mailing of notice to the Settlement Class, opting out of or objecting to the proposed Settlement, and filing papers in connection with the Final Fairness Hearing; and

(14) Appointment of Plaintiffs as Representative Settlement Class Plaintiffs and Plaintiffs' Counsel as Class Counsel for the Settlement Class.

4.

Defendant has no objection to this motion, and consents to the relief sought by Plaintiffs.

MEMORANDUM IN SUPPORT

Plaintiffs present this Memorandum in Support of their Unopposed Motion for Preliminary Approval of Proposed Settlement Agreement. Defendant does not object to this Motion and consents to the relief sought by Plaintiffs.

I. Introduction.

This Motion seeks preliminary approval of the proposed Settlement Agreement reached by the Parties to settle this class action involving the breach of Premera's computer systems that was publicly disclosed on March 17, 2015 (the "Data Breach"). The proposed Settlement includes a \$32 million Qualified Settlement Fund that will be used to make cash payments and to provide robust Credit Monitoring and Insurance to proposed Class Members who submit valid claims. Additionally, the Settlement requires Premera to spend \$42 million over three years on comprehensive remedial measures and injunctive relief in the form of business practice changes and future commitments related to Premera's IT security practices.

Plaintiffs allege that Premera was negligent, breached its contracts, and violated the Washington Consumer Protection Act ("CPA") (RCW § 19.86.020) and California's Confidentiality of Medical Information Act ("CMIA") (Cal. Civ. Code §§56.36, 56.101(a)) when it failed to prevent Plaintiffs' confidential information, including personally identifying information ("PII") and protected health information ("PHI"), and "medical information" as that term is defined under the CMIA, (collectively "Personal Information"), from being compromised in the Data Breach.

The proposed class consists of all persons in the United States whose Personal Information was stored on Premera's computer network systems that were compromised in the Data Breach. There are approximately 10.6 million class members.

The proposed Settlement Agreement is an outstanding result, reached through numerous arm's-length negotiations after heavily-contested litigation by experienced and well-informed counsel. Because the proposed Settlement is fair, reasonable and adequate, it merits preliminary approval.

II. Procedural Background.

Plaintiffs filed their respective complaints between March 18, 2015 and July 21, 2017 after they learned of the Data Breach. The Judicial Panel on Multidistrict Litigation consolidated the various cases in this Court between June and September 2015. During the course of the litigation, the Parties engaged in significant discovery. Defendant produced over 1.5 million pages of documents and the Parties collectively took more than 50 depositions. The Parties also sought the Court's guidance on several discovery disputes, including motions regarding Defendant's privilege logs, which resulted in the appointment of a Special Master, several hearings, and two published decisions.

Before reaching this Settlement, the Parties fully briefed Plaintiffs' Motion for Class Certification, as well as several motions to exclude various expert testimony. ECF 156–168, 190, 195–197, 211–219, 222–227, 247, 260–264. The Court heard the motions on November 18, 2018.

Over the course of the last several months, and while the Court's decision on these Motions was pending, the Parties engaged in extensive, arm's-length settlement negotiations, including three sessions of mediation, with the aid of the Honorable Jay C. Gandhi (Ret.) of JAMS and with

the additional aid of Peter K. Rosen, Esq. of JAMS for two of the sessions,¹ and multiple follow up emails and telephone conferences with Judge Gandhi and Mr. Rosen. On February 15, 2019, the Parties reached a preliminary agreement on the terms of a nationwide settlement. Numerous additional negotiations occurred relating to finalizing the Settlement Agreement. The proposed Settlement Agreement was executed by all Parties on May 29, 2019.

III. Terms of the Proposed Settlement.

The terms of the proposed Settlement are summarized briefly below. The full terms are set forth in the proposed Settlement Agreement.

A. Class Definition. The proposed Settlement Class is defined as:

“All persons in the United States whose Personal Information was stored on Premera’s computer network systems that was compromised in the Security Incident as publicly disclosed on March 17, 2015. Excluded from the Settlement Class are: (1) the Judge presiding over the Action, and members of his family; (2) the Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former officers and directors; (3) Persons who properly execute and submit a request for exclusion prior to the expiration of the Opt-Out Period; and (4) the successors or assigns of any such excluded Persons.”

(Ex. 1 (“SA”), ¶ 1.38).

B. Qualified Settlement Fund. The proposed Settlement Agreement creates a Qualified Settlement Fund of \$32 million that Defendant will fund to provide monetary relief to the Class, credit monitoring and insurance to the Class, attorneys’ fees and costs, Class Notice, Settlement Administration, and Service Awards. (*See SA*, at §§ III, IV, V, VI, IX.) This is a non-reversionary fund, meaning that no portion of the Qualified Settlement Fund shall revert to Premera unless this Settlement is voided, cancelled, or terminated. (*SA*, ¶ 3.7.)

¹ Two of these mediation sessions began at 10 a.m. and went well past midnight. All three of the mediation sessions included counsel for Premera’s insurance carriers.

C. Monetary Compensation. No less than \$10 million of the Qualified Settlement Fund will be used to provide direct monetary compensation to those proposed Settlement Class Members who submit valid Claim Forms. (SA, ¶ 4.2.) Each proposed Settlement Class Member may qualify for benefits and distributions from this fund as follows:

1. **Reimbursement of Out-of-Pocket Losses:** For proposed Settlement Class Members who submit Reasonable Documentation of verified unreimbursed costs or expenditures that they actually incurred, and that are plausibly traceable to the Data Breach (such as unreimbursed losses or charges due to identity theft, freezing or unfreezing of credit, credit monitoring costs, lost time, etc.), up to \$10,000. (SA, ¶ 4.3.)
2. **Default Payments:** For proposed Settlement Class Members who do not submit Reasonable Documentation of Out-of-Pocket Costs, alternative compensation of up to \$50. (SA, ¶ 4.4.)
3. **California Payments:** For proposed Settlement Class Members who, as of March 17, 2015, resided in California and who received notice from Premera that their information may have been compromised in the Data Breach, up to an additional \$50 as compensation under the California Confidentiality of Medical Information Act (“CMIA”). (SA, ¶ 4.5.)

If the approved claims in the above three categories (the “Approved Claims”) exceed the Net Qualified Settlement Fund, then the Approved Claims shall be reduced *pro rata* based on the amount of all allowed Claims. (SA, ¶ 4.2.1.) If the Approved Claims are less than the Net Qualified Settlement Fund, the excess will be used first to increase the Approved Claims on a per capita basis, and then to fund additional credit monitoring services. Finally, any residual funds not

economically viable to distribute to proposed Settlement Class Members in either of these ways will be distributed in a *cy pres* award approved by the Court. (SA, ¶ 4.7.) No amounts of the Qualified Settlement Fund shall revert to the Defendant. (SA, ¶ 3.7.)

D. Credit Monitoring and Insurance. Up to \$3.5 million of the Qualified Settlement Fund will be allocated to provide proposed Settlement Class Members with two years of Credit Monitoring and Insurance provided by Identity Guard (the “Individual Total Plan”), which provides each proposed Settlement Class Member who submits a valid Claim Form seeking to be enrolled in this service with:

1. Up to \$1 Million Dollars reimbursement insurance covering losses due to identity theft, stolen funds, etc.;
2. Three-bureau credit monitoring providing notice of changes to credit profile;
3. Authentication alerts when someone attempts to change their personal account information within the covered network;
4. High Risk Transaction Alerts providing notification of high-risk transactions including but not limited to account takeovers, wire transfers, tax refunds, payday loan applications, and cell service applications;
5. Dark Web Monitoring providing notification if their information such as Social Security number, credit card numbers, financial account numbers and/or health insurance number are found on the Dark Web;
6. Threat Alerts powered by IBM “Watson” providing proactive alerts about potential relevant threats such as breaches, phishing scams, and malware vulnerabilities;

7. Customer support and victim assistance provided by Identity Guard;
8. Anti-phishing and safe Apps for iOS and Android mobile devices; and
9. Safe browsing software for PC and Mac to help protect against malicious content with add-ons for Safari, Chrome, and Firefox web browsers that deliver proactive malware protection by blocking various malware delivery channels including phishing, malvertisements, and Flash. (The extension also blocks content and tracking cookies to help protect personal information.)

(SA, ¶ 4.6.1.) The retail value for each proposed Settlement Class Member receiving this Credit Monitoring and Insurance benefit is \$479.76 (\$19.99 per month for 24 months). *See* Identity Guard, *Total Plan*, <https://www.identityguard.com/plans/total/> (last visited May 28, 2019).

E. Business Practice Commitments. Premera agrees to provide equitable injunctive relief in the form of business practice commitments for three years from the date of final approval² of the proposed Settlement Agreement (the “Settlement Term”). These business practice commitments include a variety of methods for securing Personal Information, such as: encrypting, archiving, and maintaining protected environments for data; requiring two-factor authentication for remote access for all personnel and vendors; performing various audits and testing exercises, and collecting and maintaining logs of covered information systems; operating a Cyber Security Operations Center; employing a Chief Information Security Officer; requiring Information Security training for its associates, etc. (SA, Ex. A) (Exhibit A to the SA contains the full statement of Defendant’s business practice commitments.)

² Premera’s archiving commitment extends three years from the date it begins archiving. (SA, Ex. A.)

F. Additional Relief. In addition to the individual monetary relief, the credit monitoring and insurance, and the business practice commitments, the proposed Settlement Agreement provides the following relief to be paid from the Qualified Settlement Fund:

- 1. Payment for Notice and for Settlement Administrator:** The cost of implementing and developing a notice plan, as well as the costs of a Court-approved Settlement Administrator to disseminate notice, administer the Settlement, and evaluate and pay claims. (SA, §§ V, VI.)
- 2. Service Awards for Proposed Settlement Class Representative Plaintiffs:** In addition to any payments the proposed Representative Plaintiffs are entitled to receive for submitting valid claims, Premera has agreed to, and Class Counsel may apply to the Court for, Service Awards of up to \$5,000 to each proposed Representative Plaintiff for his or her time, effort, and risk in connection with the Action, including stepping forward to represent the proposed Class, searching for and producing data, and preparing for and sitting for their depositions. These Service Awards are not conditioned on the Plaintiffs' support of the proposed Settlement. Class Counsel negotiated the amount of Service Awards to be applied for independently from the other terms of the proposed Settlement, and the Court shall consider the Service Awards separately from its consideration and determination of the fairness, reasonableness, and adequacy of the proposed Settlement. (SA, ¶ 9.1.)
- 3. Payment of Attorneys' Fees and Expenses:** Under the proposed Settlement Agreement, and subject to Court approval, Defendant

acknowledges that Class Counsel shall be entitled to request payment of attorneys' fees and costs from the Qualified Settlement Fund. The Parties negotiated the maximum amount of the attorneys' fees, costs and expenses to be sought by Class Counsel under the supervision of the Honorable Jay C. Gandhi and Peter Rosen of JAMS, after all monetary relief terms of the proposed Settlement had been agreed upon. Prior to the Final Fairness Hearing, Class Counsel will submit a request to the Court of their attorneys' fees, reasonable costs, and expenses in an amount up to \$14 million. As that motion will make clear, the amount sought is reasonable as a percentage of the fund and is commensurate with the lodestar attorneys' fees plus expenses incurred in this matter. Premera does not and will not object, appeal, or otherwise comment upon any such attorneys' fee and expense request. (SA, ¶¶ 9.2, 9.3, 9.4, 9.6.)

G. Release of Liability. In exchange for the relief described above, Defendant will receive a full and final release of all claims related to the Data Breach that Premera publicly disclosed on March 17, 2015. (See SA, ¶¶ 1.32, 11.1 for the complete release language.)

IV. The Proposed Settlement Class Should Be Certified.

In order to grant preliminary approval of a proposed settlement, the Court should determine that the proposed settlement class is appropriate for certification. Manual for Complex Litigation ¶ 21.632 (4th ed. 2004) ("MCL 4th"); *Amchem Prods. Inc. v. Windsor*, 521 U.S. 591, 620 (1997). Class certification is proper if the proposed class, the proposed class representatives, and the

proposed class counsel satisfy the numerosity, commonality, typicality, and adequacy of representation requirements of Rule 23(a). Fed. R. Civ. P. 23(a)(1–4).

In addition to meeting the requirements of Rule 23(a), plaintiffs seeking class certification must also meet at least one of the three provisions of Rule 23(b). Fed. R. Civ. P. 23(b). When plaintiffs, such as the Plaintiffs in this action, seek class certification under Rule 23(b)(3), the representatives must demonstrate that common questions of law or fact predominate over individual issues and that a class action is superior to other methods of adjudicating the claims. Fed. R. Civ. P. 23(b)(3); *Amchem*, 521 U.S. at 615–16.

The procedure for review of a proposed class action settlement is well established. Because Plaintiffs meet all of the Rule 23(a) and 23(b)(3) prerequisites, certification of the proposed Settlement Class is proper.³

A. The Requirement of Numerosity Is Satisfied.

“The prerequisite of numerosity is discharged if ‘the class is so large that joinder of all members in impracticable.’” *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1019 (9th Cir. 1998) (quoting Fed. R. Civ. P. 23(a)(1)). A putative class of at least forty members usually is sufficient to satisfy the numerosity requirement. *Oregon Laborers-Emp’rs Health & Welfare Trust Fund v. Philip Morris, Inc.*, 188 F.R.D. 365, 372 (D. Or. 1998). At the time that the Data Breach intrusion was remediated on March 6, 2015, Premera’s network held the Personal Information of approximately 8 million current and former Premera members; approximately 1.9 million current and former non-Premera Blue Cross Blue Shield members for whom Premera administered health benefit claims; and approximately 500,000 current and former employees, providers, and vendors.

³ The Class Certification issues have been fully briefed in ECF Nos. 156–168, 190, 195–197, 218–219, 247, and 260–264, which are adopted and made part of this motion by reference.

(ECF 156, Ex. 110.) The large number of persons in the proposed Settlement Class, coupled with the fact that they are geographically disbursed throughout the country, renders joinder impracticable. *See McCluskey v. Trs. of Red Dot Corp. Emp. Stock Ownership Plan & Trust*, 268 F.R.D. 670, 674 (W.D. Wash. 2010).

B. The Requirement of Commonality Is Satisfied.

The second requirement for certification mandates that “there are questions of law or fact common to the class.” Fed. R. Civ. P. 23(a)(2). Commonality is demonstrated when the claims of all class members “depend upon a common contention . . . that is capable of class-wide resolution.” *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011). This requires that the determination of the common question “will resolve an issue that is central to the validity of each one of the claims in one stroke.” *Id.* “Even a single common question will do.” *Id.* at 359. Thus, when a defendant “has engaged in some course of conduct that affects a group of persons and gives rise to a cause of action, one or more of the elements of that cause of action will be common” and the requirements of Rule 23(a)(2) are satisfied. *Phelps v. 3PD, Inc.*, 261 F.R.D. 548, 555 (D. Or. 2009) (quoting *Oregon Laborers*, 188 F.R.D. at 373).

In this case, all proposed Settlement Class Members’ claims involve common questions of law and fact regarding Premera’s data security. Proposed Settlement Class Members’ claims arise out of a common core of facts. For example, whether Premera’s data security practices were sufficient is a common question of fact imbedded in each one of their claims. Moreover, this question would have been answered using common evidence. Premera held Personal Information for all proposed Settlement Class Members in centralized databases. ECF 156, Ex. 74 (Seymour Dep 2) at 42:8–16. Its security practices did not vary internally or among its members. Proof regarding Premera’s deficient security practices would have been common across the proposed

Settlement Class and this alone is sufficient to establish commonality. *See, e.g., Grays Harbor Adventist Christian Sch. v. Carrier Corp.*, 242 F.R.D. 568 572 (W.D. Wash. 2007) (finding numerous common questions related to Washington CPA claim); *Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2017 WL 1044692 (M.D. Ala Mar. 17, 2017), *on reconsideration in part*, 2017 WL 3816722 (M.D. Ala. Aug. 31, 2017) (holding, in data breach case, that “[t]he effect and terms of the purported contract are common points sufficient to carry the first claim past Rule 23(a)(2)”).

Additional common questions include: (1) Whether Premera was aware or had reason to be aware that its systems were vulnerable to attack, given multiple government warnings and the inadequacies and deficiencies in its own data security policies and procedures; (2) whether Premera violated HIPAA in its policies and practices regarding data security; (3) whether Premera was unfair or deceptive in its business practices by failing to disclose deficiencies in its data security; (4) whether the Data Breach compromised Personal Information; and (5) whether the proposed Settlement Class Members would be entitled to damages as a result of Premera’s conduct. These common questions run throughout all claims of the proposed Settlement Class and satisfy the commonality requirement of Rule 23.

C. The Requirement of Typicality Is Satisfied.

Rule 23 next requires that the class representatives’ claims be typical of those of the class members. Fed. R. Civ. P. 23(a)(3). “The purpose of the typicality requirement is to assure that the interest of the named representative aligns with the interests of the class.” *Hanon v. Dataproducts Corp.*, 976 F.2d 497, 508 (9th Cir. 1992). “The test of typicality is whether the other members have the same or similar injury, whether the action is based on conduct which is not unique to the named plaintiffs, and whether other class members have been injured in the same course of

conduct.” *Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 984 (9th Cir. 2011). The Ninth Circuit does not require the named plaintiffs’ injuries to be “identical with those of the other class members, [but] only that the unnamed class members have injuries similar to those of the named plaintiffs and that the injuries result from the same injurious course of conduct.” *Armstrong v. Davis*, 275 F.3d 849, 869 (9th Cir. 2001), *abrogated on other grounds by Johnson v. California*, 543 U.S. 499, 504–05 (2005)). Thus, “a plaintiff’s claim is typical if it arises out of the same event or practice or course of conduct that gives rise to the claims of other class members and his or her claims are based on the same legal theory.” *Phelps*, 261 F.R.D. at 557 (quoting *Sorenson v. Concanon*, 893 F. Supp. 1469, 1479 (D. Or. 1994)). In addition, at least one class representative must have standing to pursue claims against Defendant in order for the typicality prong to be met. *See In re Abbott Labs. Norvir Anti-Trust Litig.*, No. C 04–1511 CW, 2007 WL 1689899, at *3 (N.D. Cal. June 11, 2007) (“[I]t is well-settled that prior to the certification of a class, and technically speaking before undertaking any formal typicality or commonality review, the district court must determine that at least one named class representative has Article III standing to raise each class subclaim.” (quotation marks omitted)); *see also Frank v. Gaos*, ___ U.S. ___, 139 S. Ct. 1041, 1046 (2019) (“A court is powerless to approve a proposed class settlement if . . . no named plaintiff has standing.”).

Plaintiffs’ claims and the Settlement Class Member’s claims arise from the same conduct by Premera. Plaintiffs are each typical of the proposed Settlement Class because Plaintiffs possess the same interests and suffered harm from the same conduct as did the proposed Settlement Class Members. Plaintiffs and the proposed Settlement Class Members each had Personal Information that was stored on Premera’s computer network systems when those systems were compromised in the Data Breach. And each of the named Plaintiffs has standing to pursue their claims. It is well-

established in the Ninth Circuit that an increased risk of harm for victims of data theft, where the data taken is sensitive and personal (such as the Personal Information here), and where Plaintiffs allege at least some information has been used for harm, as Plaintiffs allege here, meets the requirements for Article III standing. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018), *cert. denied sub nom. Zappos.com, Inc. v. Stevens*, 139 S. Ct. 1373 (2019). Thus, Plaintiffs' claims arise out of the same course of conduct, are based on the same legal theories, seek the same types of damages as the proposed Settlement Class, and meet all necessary standing requirements. Accordingly, the typicality requirement is satisfied.

D. The Requirement of Adequate Representation Is Satisfied.

The final Rule 23(a) prerequisite requires that the proposed class representatives have and will continue to "fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a)(4). "To determine whether named plaintiffs will adequately represent a class, courts must resolve two questions: '(1) do the named plaintiffs and their counsel have any conflicts of interest with other class members and (2) will the named plaintiffs and their counsel prosecute the action vigorously on behalf of the class?'" *Ellis*, 657 F.3d at 985 (quoting *Hanlon*, 150 F.3d at 1020).

Here, the interests of the Plaintiffs are identical to the interests of each member of the proposed Settlement Class since they each had Personal Information stored on Premera's computer network systems when those systems were compromised in the Data Breach, and they each seek to recover damages and injunctive relief related to the Data Breach. Plaintiffs have no interests that are antagonistic to or in conflict with the persons in the proposed Settlement Class they seek to represent, and they have a substantial interest in the outcome of this action, since their Personal Information was compromised in the Data Breach. In addition, proposed Class Counsel are active practitioners with substantial experience in consumer, privacy and data breach litigation, who have

been appointed to leadership positions in numerous class actions. *See* Declarations filed with Plaintiffs’ Motion for Class Certification: ECF 157 (Declaration of Keith S. Dubanevich at ¶¶ 3–9); ECF 158 (Declaration of James J. Pizzirusso at ¶¶ 2–4); ECF 159 (Declaration of Karen Hanson Riebel at ¶¶ 3–5); ECF 161 (Declaration of Kim D. Stephens at ¶¶ 2–4); ECF 162 (Declaration of Tina Wolfson at ¶¶ 11–18). The requirements of Rule 23(a) are satisfied.

E. The Proposed Settlement Meets the Requirements of Rule 23(b)(3).

Once the threshold requirements of Rule 23(a) are satisfied, Plaintiffs also must show that “questions of law and fact common to the members of the class predominate over any questions affecting only individual members,” and that a class action is superior to other available methods of adjudicating the claims. Fed. R. Civ. P. 23(b)(3). Rule 23(b)(3)’s predominance requirement tests whether proposed classes are “sufficiently cohesive to warrant adjudication by representation.” *Hanlon*, 150 F.3d at 1022 (citing *Amchem*, 521 U.S. at 623). The predominance inquiry measures the relative weight of the common questions as against individual ones. *Amchem*, 521 U.S. at 624. Common issues predominate here because Plaintiffs contend the central liability question in this case—whether Premera’s Security Incident wrongfully exposed the proposed Settlement Class’s Personal Information to compromise—can be established through generalized evidence.

1. Common Issues of Law and Fact Predominate in All Four Causes of Action.

The proposed Settlement seeks to resolve four factually related causes of action: CPA, Negligence, Breach of Contract, and CMIA. Each of these claims rests on the same factual basis: Defendant held the proposed Settlement Class Members’ Personal Information on its computer systems; Defendant had a duty to safeguard this Personal Information; Defendant failed in that

duty and thereby permitted Members' Personal Information to be compromised in the Data Breach; and the proposed Settlement Class Members were harmed by this exposure of their Personal Information. The common factual and legal issues overwhelmingly predominate over individualized concerns in a case like this one where the proposed Settlement Class Members were all allegedly damaged by the same conduct with respect to Defendants' centralized computer systems.

The Court must analyze choice of law as part of the predominance inquiry. *See Mazza v. Am Honda Motor Co., Inc.*, 666 F.3d 581, 589–90 (9th Cir. 2012). Here, the aggregated contacts with the State of Washington overwhelmingly point to the application of Washington law for the CPA and Negligence Claims. Restatement (Second) of Conflict of Laws § 145; *Pruczinski v. Ashby*, 374 P.3d 102, 108 n.7 (Wash. 2016). Premera's place of incorporation and principal place of business is Washington. Premera stored the proposed Settlement Class members' data on servers in Washington and all of Premera's data security conduct occurred in Washington. "[T]he place where the defendant's conduct occurred will usually be given particular weight in determining the state of the applicable law." *Id.* § 145 cmt. e. In other nationwide data breach cases, courts have applied similar reasoning. *In re Target Corp. Customer Data Sec. Breach Litig.*, 309 F.R.D. 482, 489 (D. Minn. 2015) (holding that Minnesota law applied to all class members' negligence claims because Target was incorporated and headquartered in Minnesota; the relevant servers affected by the breach were in Minnesota; security decisions were made in Minnesota; and Target employees' failure to heed specific warnings about security vulnerabilities occurred in Minnesota); *see also Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d at 1153–54 (finding Washington had most significant relationship where misconduct related to defendant's decisions concerning internal data security that led to a data breach were made "at its corporate

headquarters in Bellevue, Washington,” and its failure to employ adequate data security measures “emanated from [its] headquarters” even though plaintiff was located in Iowa).

With respect to the Breach of Contract Claim, there is no meaningful difference in the relevant law among the various states, so the Court does not need to make a choice of law decision. Breach of contract claims are based on black letter common law that does not materially vary among the implicated states. *See, e.g., In re U.S. Foodservice Inc. Pricing Litig.*, 729 F.3d 108, 127 (2d. Cir. 2013) (“A breach is a breach is a breach, whether you are on the sunny shores of California or enjoying a sweet autumn breeze in New Jersey.” (citation omitted)).

Finally, the CMIA Claim is a California state law claim that, by its terms and the terms of the proposed Settlement, will only impact the proposed Settlement Class Members who resided in California as of March 17, 2015, the date Premera gave notice of the Data Breach. Premera knowingly insured individuals who resided in California; it was therefore aware that it could be subject to California’s additional statutory requirements for California residents. While Premera’s conduct was centered in Washington, California has a significant relationship to the dispute with respect to the legal protections California established under the CMIA. California has the most significant relationship with respect to this particular claim (that does not exist under Washington or Oregon law), and California has a clear interest in ensuring that its citizens are protected by the provisions of the CMIA. Restatement (Second) of Conflict of Laws § 145.

Applying these choice of law principles to each of the four causes of action resolved in this proposed Settlement Agreement, it is clear that common issues of law and fact predominate over individualized concerns.

a. Common Issues of Law and Fact Predominate for the Washington CPA Claim.

With respect to the Washington CPA Claim, Plaintiffs have asserted that they are entitled to recover damages because Premera's failure to provide adequate data security for their Personal Information was an unfair practice that violated the CPA. Plaintiffs have also asserted that Premera's failure to inform class members, employers, or regulators that it lacked appropriate data security was a deceptive practice that violated the CPA. "To establish a CPA violation, the plaintiff must prove five elements: (1) an unfair or deceptive act or practice that (2) occurs in trade or commerce; (3) impacts the public interest; (4) and causes injury to the plaintiff in her business or property, and (5) the injury is causally linked to the unfair or deceptive act." *Michael v. Mosquera-Lacy*, 200 P.3d 695, 698–99 (Wash. 2009) (citing *Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co.*, 719 P.2d 531, 533 (Wash. 1986)); RCW § 19.86.020. Plaintiffs would prove each of these elements by generalized proof regarding whether Premera's data security was adequate and the actual vulnerabilities of the Personal Information stored within Premera's computer systems, the facts of the breach of those systems, and the resulting exposure of the proposed Settlement Class Members' data and caused damages. The Washington CPA applies extraterritorially. *Thornell v. Seattle Serv. Bureau, Inc.*, 363 P.3d 587, 592 (Wash. 2015). Therefore, this Court can apply it to all proposed Settlement Class Members. Thus, common issues of law and fact predominate individualized issues with respect to the Washington CPA claim.

b. Common Issues of Law and Fact Predominate in the Negligence Claim.

To prove his or her Negligence Claim under Washington law, a plaintiff must show "(1) the existence of a duty, (2) breach of that duty, (3) resulting in injury, and (4) proximate cause." *Ranger Ins. Co. v. Pierce Cty*, 192 P.3d 886, 889 (Wash. 2008). Again, all issues pertinent to these

claims can be resolved on a classwide basis as Plaintiffs' liability case depends first and foremost on whether Premera used adequate data security practices to protect class members' Personal Information. The duty would be the duty Premera owed to proposed Settlement Class members to maintain adequate data protection over the Personal Information within its computer systems; the breach of the duty would be Premera's failure to adequately safeguard those systems; and proximate cause would be shown in the relationship of the Data Breach to Defendant's failure to appropriately safeguard its systems. Again, these joint questions would overwhelmingly predominate over individualized inquiries.

c. Common Issues of Law and Fact Predominate in the Breach of Contract Claim.

Plaintiffs' contract claim is based on promises Premera made in the Notice of Privacy Practices it sent to its members. This Notice included identical promises to all proposed Settlement Class Members that Premera is "committed to maintaining the confidentiality of your medical and financial information," "must take measures to protect" members' data, and "take steps to secure [its] buildings and electronic systems from unauthorized access." ECF 156, Exs. 5, 6. The joint issues of fact and law inherent in this claim include the question whether this Notice was incorporated by reference into the members' contracts, as Premera had a uniform practice of mailing the notice along with the policy booklet contract. ECF 156, Ex. 7; *see also In re Premera Blue Cross Consumer Data Sec. Breach Litig.*, No. 3:15-md-2633-SI, 2017 WL 539578, at *10–11 (D. Or. Feb. 9, 2017) (citing *Dalmage v. Combined Ins. Co. of Am*, No. 14 C 3809, 2016 WL 754731, at *4–6 (N.D. Ill. Feb. 23, 2016)) (holding that concurrent receipt of the Privacy Notice with the policy booklet was sufficient to state a claim for breach of contract based on the Privacy Notice.).

The claim for breach of a “form contract . . . present[s] the classic case for treatment as a class action.” *In re Scotts EZ Seed Litig.*, 304 F.R.D. 397, 411 (S.D.N.Y. 2015); *see also In re U.S. Foodservice Inc. Pricing Litig.*, 729 F.3d 108, 124 (2d Cir. 2013) (affirming class certification where, as here, each proposed class member was subject to the same material contractual terms). Thus, common issues greatly predominate individualized concerns with respect to the Breach of Contract Claim.

d. Common Issues of Law and Fact Predominate in the CMIA Claim.

California’s Confidentiality of Medical Information Act prohibits covered entities such as Premera from negligently releasing an individual’s confidential medical information and obligates a covered entity to treat such medical information in a “manner that preserves the confidentiality of the information contained therein.” Cal. Civ. Code §§ 56.36, 56.101(a); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1201 (D. Or. 2016). To establish a violation of the CMIA, a plaintiff must show that the defendant negligently caused the release of “individually identifiable information . . . regarding a patient’s medical history, mental or physical condition, or treatment,” and that an unauthorized third party “viewed or otherwise accessed” the confidential information. Cal. Civ. Code § 56.05(j); *Regents of the Univ. of Cal. v. Superior Court*, 220 Cal. App. 4th 549, 554, 564–65, 163 Cal. Rptr. 3d 205, 208, 216 (2013). This claim applies only to those proposed Settlement Class Members who resided in California prior to March 17, 2015 while they were Premera-insureds. The question of whether a proposed Settlement Class Member is eligible for damages under the CMIA is easily resolved by asking each proposed Settlement Class member the same question: whether they resided in California at the relevant time.

Premera's alleged violations of the CMIA affected all proposed Settlement Class members who resided in California at the relevant time in materially the same way. Premera had in its computer systems individually identifiable information relating to their medical history, condition, or treatment. ECF 156, Ex. 74 (Seymour Depo. 2 at 42:8–16). The privacy of their medical information was compromised in the same way during the Data Breach. CMIA claims resulting from the failure to adequately protect medical information have been certified as a class action for settlement. *See Johansson-Dohrmann v. Cbr Sys., Inc.*, 12-CV-1115-MMA BGS, 2013 WL 3864341, at *8 (S.D. Cal. July 24, 2013). Thus, once again, the common issues of law and fact would predominate over individualized concerns with respect to the CMIA Claim.

2. Class Adjudication Would Be Superior to Other Available Methods.

“[T]he purpose of the superiority requirement is to assure that the class action is the most efficient and effective means of resolving the controversy” 7AA Charles Wright, Arthur Miller & Mary Kay Kane, *Federal Practice and Procedure* § 1779 (3d ed. 2005); *Wolin v. Jaguar Land Rover N. Am., LLC*, 617 F.3d 1168, 1175 (9th Cir. 2010). “Rule 23(b)(3)’s superiority test requires the court to determine whether maintenance of this litigation as a class action is efficient and whether it is fair. This analysis is related to the commonality test. Underlying both tests is a concern for judicial economy.” *Id.* at 1175–76.

“‘Where damages suffered by each putative class member are not large,’ the first factor ‘weighs in favor of certifying a class action.’” *Agnes v. Papa John’s Int’l, Inc.*, 286 F.R.D. 559, 571 (W.D. Wash. 2012) (quoting *Zinser v. Accufix Research Inst., Inc.*, 253 F.3d 1180, 1190 (9th Cir. 2001)). “The policy ‘at the very core of the class action mechanism is to overcome the problem that small recoveries do not provide the incentive’ for individuals to bring claims.” *Id.* (quoting *Amchem*, 521 U.S. at 617). Courts have held the superiority requirement was met even where the

amount of damages could reach \$1,500 per individual. *Kavu, Inc. v. Omnipak Corp.*, 246 F.R.D. 642, 650 (W.D. Wash. 2007); *see also Rodriguez v. Experian Info. Solutions, Inc.*, No. C15-01224-RAJ, 2018 WL 1014606, at *6 (W.D. Wash. Feb. 22, 2018) (superiority requirement met where “relatively small” statutory damages of \$1000 per violation under the Fair Credit Reporting Act would deter individual litigants).

Like other proposed class actions, this case involves millions of individual class members, each of whom have suffered a relatively small amount of damages. Even at the high end of the estimates for recovery, individual litigation would be cost-prohibitive. *See Chamberlan v. Ford Motor Co.*, 402 F.3d 952, 960 (9th Cir. 2005) (“[T]he district court did not abuse its discretion in finding that, absent a class action, Class Plaintiffs would have no meaningful redress . . .”). Here, litigating through a class action is superior to leaving Plaintiffs and the proposed class members without a viable means of pursuing their claims.

Because the claims are being certified for purposes of settlement, there are no manageability issues. *Amchem*, 521 U.S. at 620 (“Confronted with a request for settlement-only certification, a district court need not inquire whether the case, if tried, would present intractable management problems . . . for the proposal is that there be no trial.”). Additionally, the resolution of hundreds of thousands of claims in one action is far superior to individual lawsuits and promotes consistency and efficiency of adjudication. *See id.* at 617 (noting the “policy at the very core of the class action mechanism is to overcome the problem that small recoveries do not provide the incentive for any individual to bring a solo action prosecuting his or her rights.”). Certification for purposes of settlement is appropriate.

V. The Court Should Appoint Plaintiffs’ Counsel as Class Counsel.

After certifying a class, Rule 23 requires a court to appoint class counsel that will fairly and adequately represent the class members. Fed. R. Civ. P. 23(g)(1)(B). In making this determination, the Court must consider, *inter alia*, counsel’s (i) work in identifying or investigating potential claims; (ii) experience in handling class actions or other complex litigation and the types of claims asserted in the case; (iii) knowledge of the applicable law; and (iv) resources committed to representing the class. Fed. R. Civ. P. 23(g)(1)(A)(i–iv).

As set forth in Section IV.D. above (pp.16–17), proposed Class Counsel have extensive experience in consumer, privacy and data breach class action cases. Proposed Class Counsel have successfully litigated and settled numerous data breach class actions across the country and were extremely well qualified to litigate this case. In addition, proposed Class Counsel have spent almost four years litigating this case, conducting discovery, and advocating for the class. As a result of their efforts, the negotiated proposed Settlement provides considerable monetary and equitable relief to each of the proposed Settlement Class members. (*See* Section III. above, pp. 6–11.) Thus, this Court should appoint Kim D. Stephens and Jason T. Dennett of Tousley Brain Stephens PLLC; Keith S. Dubanevich of Stoll Berne; Tina Wolfson of Ahdoot and Wolfson, PC; James Pizzirusso of Hausfeld LLP; and Karen Hanson Riebel of Lockridge Grindal Nauen P.L.L.P. as Class Counsel.

VI. The Proposed Settlement Is Fundamentally Fair, Reasonable, and Adequate, and thus Warrants Preliminary Approval.

The Court should also grant preliminary approval of the proposed Settlement. A court’s ultimate approval of a class action settlement involves the consideration of certain factors to determine whether a proposed settlement is fair, reasonable, and adequate. Fed. R. Civ. P. 23(e)(2).

Preliminary approval of a settlement is appropriate if “the proposed settlement appears to be the product of serious, informed, non-collusive negotiations, has no obvious deficiencies, does not improperly grant preferential treatment to segments of the class, and falls within the range of possible approval.” *See Booth v. Strategic Realty Trust, Inc.*, No. 13–cv–04921–JST, 2015 WL 3957746, at *6 (N.D. Cal June 28, 2015) (citing *In re Tableware Antitrust Litig.*, 484 F. Supp. 2d 561, 570 (E.D. Pa. 2001); *see also* MCL 4th § 21.632. “To assess a settlement proposal, courts must balance the strength of the plaintiffs’ case; the risk, expense, complexity, and likely duration of further litigation; the risk of maintaining class action status throughout the trial; the amount offered in settlement; the extent of discovery completed and the state of the proceedings; the experience and views of counsel; the presence of a governmental participant; and the reaction of the class members to the proposed settlement.” *In re Online DVD-Rental Antitrust Litig.*, 779 F.3d 934, 944 (9th Cir. 2015).

Importantly, this Motion seeks preliminary approval of the proposed Settlement, not final approval. Accordingly, the standards are not as stringent as those applied to a motion for final approval. MCL 4th § 21.63 (“At the stage of preliminary approval, the questions are simpler, and the court is not expected to, and probably should not, engage in analysis as rigorous as is appropriate for final approval.”). If the proposed Settlement discloses no reason to doubt its fairness, has no obvious deficiencies, does not improperly grant preferential treatment to class representatives or segments of the class, does not grant excessive compensation to attorneys, and appears to fall within the range of possible approval, the Court should grant preliminary approval. For the following reasons, this proposed Settlement should be preliminarily approved.

A. The Proposed Settlement Agreement Is the Product of Serious, Informed, and Non-Collusive Negotiations.

The Court’s role is to ensure that “the agreement is not the product of fraud or overreaching by, or collusion between, the negotiating parties, and that the settlement, taken as a whole, is fair, reasonable and adequate to all concerned.” *Hanlon*, 150 F.3d at 1027; *see also In re Online DVD*, 779 F.3d at 944 (noting settlements in class actions “present unique due process concerns for absent class members,” including the risk that class counsel “may collude with the defendants” (quoting *In re Bluetooth Headset Prods. Liab. Litig.*, 654 F.3d 935, 946 (9th Cir. 2010))).

The Court may presume that a proposed settlement is fair and reasonable when it is the result of arm’s-length negotiations. 4 Newberg on Class Actions ¶ 11.41 (4th ed). In this case, there is no evidence the settlement involves fraud or collusion. In addition, there is also a presumption that no fraud or collusion occurred between counsel, in the absence of any evidence to the contrary. *Id.*

The proposed Settlement is the result of intensive, arm’s-length negotiations between experienced attorneys for all Parties who are familiar with class action litigation in general and with the legal and factual issues of this case in particular. *See* Dubanevich Decl., Ex. B, ¶¶ 7–10. Plaintiffs’ Counsel are particularly experienced in the litigation, certification, trial, and settlement of data breach class actions. *See* Section IV.D. above (pp.15–16). As detailed in Section II above (p. 5), the Settlement was the result of months of extensive and arm’s-length settlement negotiations, including three extended mediation sessions with the aid of Judge Gandhi and Mr. Rosen, Esq. On February 15, 2019, the Parties reached a preliminary agreement on terms for a nationwide settlement. All the Parties executed the proposed Settlement Agreement on May 29, 2019. A settlement negotiated with the assistance of an experienced private mediator is further

proof that the settlement was reached fairly and provides adequate relief to the class. *In re Bluetooth Headset Prods. Liab. Litig.*, 654 F.3d at 948 (recognizing that use of a mediator is “a factor weighing in favor of a finding of non-collusiveness”).

Plaintiffs’ Counsel spent years engaging in written discovery, document review, depositions, data analysis, expert analysis, and analyzing legal issues related to the lawsuit’s claims. *See* Dubanevich Decl., Ex. B, ¶ 3; *Hanlon*, 150 F.3d at 1027 (no basis to disturb the settlement in the absence of any evidence suggesting that the settlement was negotiated in haste or in the absence of information). Plaintiffs and proposed Class Counsel support the settlement as fair, reasonable, adequate and in the best interests of the members of the proposed Settlement Class. This factor favors granting preliminary approval.

B. Complexity, Expense, and Likely Duration of the Litigation.

Class action cases present many complex issues. The unique legal questions raised in this case were extremely complex. At this point in the litigation, the Parties have engaged in substantial discovery that produced 1.5 million pages of documents relating to the claims of the Plaintiffs and the proposed Settlement Class. The case has been pending for almost four years. The complexity of this case is apparent not only from the issues involved, but also from the extensive record.

This litigation, including the settlement negotiations, has been complex, expensive and time-consuming for all Parties. Further litigation would be prolonged and expensive with unknown results. The proposed Settlement avoids these risks and provides immediate and certain relief to the proposed Settlement Class. This factor weighs in favor of preliminary approval.

C. The Stage of the Proceedings and the Amount of Discovery Completed Support Preliminary Approval.

Plaintiffs' Counsel have thoroughly analyzed the factual and legal issues involved in this case. Plaintiffs' Counsel's investigation of the Data Breach and Premera's data security practices commenced in 2015. Since that time, proposed Class Counsel have fully defended against and survived Premera's two motions to dismiss, reviewed over a million pages of documents during a lengthy discovery period, taken and defended more than 50 depositions, including those of eight experts, filed and argued numerous discovery motions, and fully briefed their motion for class certification and motions to exclude expert testimony. Through this extensive discovery, Plaintiffs' Counsel obtained essential information about the Data Breach and Premera's data security practices. Plaintiffs' Counsel also retained four experts to measure damages, investigate the Data Breach, and conduct forensic analysis of Premera's computer and data systems. This factor favors preliminary approval of the proposed Settlement.

D. The Proposed Settlement Provides Substantial Relief to the Proposed Settlement Class and Treats All Proposed Settlement Class Members Fairly.

As detailed above, the terms of the proposed Settlement are extremely fair to all proposed Settlement Class Members. *See* pp. 4–9, *supra*. Premera agrees to pay \$32 million to fund a Qualified Settlement Fund. As explained in more detail below, the Qualified Settlement Fund will provide Settlement Class Members with substantial individual monetary relief and robust Credit Monitoring and Insurance worth hundreds of dollars per claimant. Premera commits to a variety of injunctive measures to protect Settlement Class Members data stored in its systems in the future, and has committed to investing no less than \$14 million per year for three years on these efforts. The Qualified Settlement Fund also will be used to pay any class representative Service Awards,

attorneys' fees to proposed Class Counsel, and notice and claims administration costs, as approved by the Court. (SA, §§ III, IV, V, IX.) The Qualified Settlement Fund is non-reversionary, ensuring that the monetary benefits will go to the proposed Settlement Class—any residual Settlement Funds will be distributed first, to the extent feasible, as additional compensation or Credit Monitoring and Insurance services to the Class, and to the extent not feasible for such distribution, to an appropriate *cy pres* recipient, to be approved by the Court. (SA ¶ 4.7.1(c).)

1. The Credit Monitoring and Insurance Services Provide Valuable Benefits to Settlement Class Members.

The Settlement Agreement provides Settlement Class Members with two years of Credit Monitoring and Insurance Services through Identity Guard. The services offered to the Settlement Class Members have a retail value of \$19.99 per month per individual. *See supra* Section III.D.; Identity Guard, *Total Plan*, <https://www.identityguard.com/plans/total/> (last visited May 28, 2019). Over the two-year period that the Settlement Agreement provides this service, this amounts to a value of \$479.76 for each participating Settlement Class Member. Given a class size of approximately 10.6 million individuals, this is an enormous benefit, potentially amounting to hundreds of millions of dollars of savings to Settlement Class Members were they to obtain similar, or even inferior, credit-monitoring products on their own on the open market. A higher response rate means more claimants will receive the Credit Monitoring and Insurance Services, resulting in an increase in the value attributable to that component of the Settlement. Thus, the actual value of the benefits to the Settlement Class Members includes, for every 1% of Settlement Class Members that receive this service, an additional value to the Settlement Class of approximately \$50,854,560.00, before excluding the cost of the Credit Monitoring and Insurance Services.

The retail value of these services (rather than the cost) is the proper gauge to apply here, given that this represents the value of the benefit Class Members will actually receive. *See, e.g., Johansson-Dohrmann v. Cbr Sys., Inc.*, No. 12-cv-1115-MMA (BGS), 2013 WL 3864341, at *9 (S.D. Cal. July 24, 2013) (including value of credit monitoring in value of common fund, and finding requested fees “well within the 25% benchmark”);⁴ *In re The Home Depot, Inc. Customer Data Sec. Breach Litig.*, No.: 1:14-md-02583-TWT, 2016 WL 6902351, at *4 (N.D. Ga. Aug. 23, 2016) (granting final approval and reasoning that “[t]hese services have a retail value of approximately \$180 per enrollee”); *Lockwood v. Certegy Check Servs., Inc.*, No. 07-cv-01434, Dkt. 101 at 9 n.4 (M.D. Fla. Sept. 3, 2008) (“Using the Representative Plaintiffs’ estimates of the value of the monitoring”); *In re Michaels Stores Pin Pad Litig.*, No. 11-cv-03350, Dkts. 103 (fee motion), 107 (final approval order) (N.D. Ill. Mar. 3 & Apr. 17, 2013) (granting fee request justified under percentage method based on retail value of credit monitoring); *In re Experian Data Breach Litig.*, No. 8:15-cv-01592-AG-DFM (C.D. Cal. May 10, 2019), Dkt. 322 (final approval order) at 2 (granting fee request justified under percentage method based on retail value of credit monitoring).

2. Premera’s Investment in Injunctive Measures Provides Additional Value to the Class.

Premera agreed to spend \$42 million on improved data security between 2019 and 2022. Settlement Agreement Exhibit A and Paragraph 4.8.2; Declaration of Robert Vigil (“Vigil Decl.”) at ¶¶ 18–21; 26–28. This improved data security benefits everyone whose data is in Premera’s system because a new data breach would cause harm to those people. *Id.* at ¶¶ 9–10 (citing

Declaration of Dr. Coleman Bazelon In Support of Plaintiffs’ Motion For Class Certification, ECF 164 at ¶ 19).

Premera agrees that its cost to obtain and maintain the components of the injunctive relief is equal to the difference between (1) the \$14 million per year Premera is obligated to spend on data security under the Settlement Agreement and (2) Premera’s pre-breach IT security budget.⁵ SA ¶ 4.8.2. Dr. Vigil calculates that cost, then values the benefit to the class members using the Cost Approach, a conservative and commonly used method to value an intangible asset like data security. Vigil Decl. at ¶¶ 18–20; 10–17.

The Cost Approach is a methodology that is commonly used by economists and finance professionals to value many different types of assets. *Id.* at ¶ 11. This approach is most applicable in situations, similar to this case, where cost information is known, the intangible asset being valued is new (*i.e.*, the improvement in data security), and the type of value being estimated is the value in continued use by the current owner. *Id.* at ¶ 12. The premise of the Cost Approach is that “the cost to purchase or develop [an asset] is commensurate with the economic value of the service that the [asset] can provide during its life.” *Id.* at ¶ 16, citing Smith, Gordon V., and Russell L. Parr, *Valuation of Intellectual Property and Intangible Assets* 197–98 (3d ed. 2000). Inherent in Premera’s decision to spend money on data security is a belief that its customers will benefit by an amount *at least as much* as it spends. Premera may believe that its customers will benefit by more than what it spends, but not less. If Premera did not believe its customers would benefit by the amount it has already spent and has agreed to spend, it would not be rational for Premera to spend this money. *Id.* at ¶ 17. Courts have found the Cost Approach to be an acceptable valuation

⁵ To protect Premera’s confidentiality, Premera’s historical IT budgets and patient population data are detailed only in Dr. Vigil’s report, which the parties will move to file under seal.

methodology in a wide variety of cases. *See, e.g., Apple, Inc. v. Samsung Elecs. Co., Ltd.*, No.: 12–CV–00630–LHK, 2014 WL 794328 at *4-5, 11 (N.D. Cal. Feb. 25, 2014) (valuing patents related to various smartphone features); Vigil Decl. at ¶ 15 (compiling additional cases).

However, the improved data security benefits not just class members (those whose data was in Premera’s system at the time of the breach) but also those people whose data was added to that database between the breach and the present. Dr. Vigil adjusted the value to the class considering the number of people added to Premera’s database between the data breach and the present and estimating the increase during the three year injunctive period. *Id.* at ¶¶ 21–24. Based on that calculation, the value to the class members of the injunctive relief that Premera has agreed to pay for and implement over the three-year settlement period is, at least, **\$11,872,000**. Vigil Decl. at ¶¶ 3; 23–25.

Premera agrees that plaintiffs and Class Counsel were a catalyst in causing Premera to undertake remedial IT security measures it has already undertaken. Settlement Agreement ¶ 4.8.2. Those investments have already benefitted the class members in the form of improved security. Dr. Vigil calculated the value to the class members of the additional data security practices that Premera implemented from 2015 to 2018 at **\$30,104,000**. Vigil Decl. at ¶¶ 3; 30–32.

E. The Proposed Settlement Is Fair and Reasonable in Light of the Alleged Claims and Defenses.

Plaintiffs and Plaintiffs’ Counsel were confident in the strength of their case, but also pragmatic in their evaluation of the risks in continued litigation and the various defenses advanced by Premera. Proposed Settlement Class Members could have ended up recovering only a fraction of the proposed Settlement Agreement benefits, or losing the case at or before trial and recovering nothing at all. The Parties asked the Court to stay any ruling on class certification to allow for

mediation to take place. If mediation was unsuccessful, the Parties anticipated a ruling from the Court on class certification. The risks of an adverse ruling on class certification, or at trial, were considerable. In addition, Premera filed a Motion for Partial Summary Judgment on issues related to the filed rate doctrine, which is still pending as of the date of this Settlement, posing additional risk to some of Plaintiffs' claims.

The proposed Settlement provides certain and substantial relief to the proposed Settlement Class without delay and is within the range of reasonableness, particularly in light of the risks the Plaintiffs would face in continued litigation.

VII. The Proposed Notice Plan Should be Approved.

To satisfy the requirements of both Rule 23 and due process, Rule 23(c)(2)(B) provides that, "[f]or any class certified under Rule 23(b)(3), the court must direct to class members the best notice that is practicable under the circumstances, including individual notice to all members who can be identified through reasonable effort." Fed. R. Civ. P. 23(c)(2)(B); *Eisen v. Carlisle & Jacquelin*, 417 U.S. 156, 173 (1974). Rule 23(e)(1) similarly requires that notice be reasonably disseminated to those who would be bound by the court's judgment. Fed. R. Civ. P. 23(e)(1). The best practicable notice is that which is "reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections." *Mullane v. Cent. Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950).

Defendant has agreed to provide—within thirty days of the date of the Order preliminarily approving this proposed Settlement ("Preliminary Approval Order")—a list in electronic form of persons that, according to its records, may be proposed Settlement Class Members including to the extent available in Premera's records each proposed Settlement Class Member's most current email and mailing address. (SA, ¶ 6.2.1.) At the same time, Premera has agreed to provide a list in

electronic form of persons that, according to its records, previously received written notice of the Data Breach, along with the email and mailing address used at the time such notice was sent. *Id.*

The proposed forms of notice, the Summary Notice and the Long Form Notice (SA, ¶ 6.1.4 and SA, Exhibits B and C) (“Notices”), satisfy all of the criteria of Rule 23. The Notices are clear, straightforward, and provide persons in the proposed Settlement Class with enough information to evaluate whether to participate in the proposed Settlement. The Notices also advise the proposed Settlement Class on how to object to the settlement, including Plaintiffs’ attorney fees and costs. Thus, the Notices satisfy the requirements of Rule 23. *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 808 (1985) (explaining a settlement notice must provide settlement class members with an opportunity to present their objections to the settlement).

While Rule 23 does not require that each potential class member receive actual notice of the class action, *Mullane*, 339 U.S. at 316, the proposed Settlement Agreement provides for direct notice via either email or U.S. Mail to members of the proposed Settlement Class. The Class Member list that Premera has agreed to generate is especially trustworthy, as it is comprised entirely of individuals whose information is contained on Premera’s computer system, and whose information therefore may have been exposed in the Data Breach. Because the Parties have the ability to send direct notice to nearly 100% of all Class Members, publication notice is not necessary. But, in an abundance of caution, there will be some publication notice (still to be defined).

Besides direct-mail and email notice, the Claims Administrator will create a settlement website that will contain information for proposed Settlement Class Members and provide an opportunity for proposed Settlement Class Members to submit a claim form online. (SA, ¶ 6.2.9.) In addition, the Claims Administrator will establish a toll-free telephone number through which

Settlement Class members may obtain information about the Settlement. (SA, ¶ 6.2.11.) As an extra precaution, the proposed Settlement Agreement requires the appointment of a Notice Specialist who has recognized expertise in class action notice generally and data security litigation specifically to review the Notice and Claim Forms and assist with any recommended revisions as agreed to by the Parties and subject to this Court's approval. (SA, ¶¶ 1.19, 6.1.14, 6.2.10.)

The Parties have agreed to request the appointment of Epiq as the Settlement Administrator for this Settlement. Epiq has almost 30 years of experience serving as a Settlement Administrator in many large and complex class action lawsuits, including in other data breach lawsuits in which it handled similar duties with respect to assisting class members avail themselves of credit monitoring services, and resolving claims for out of pocket expenses. Additionally, the Parties have agreed to request the appointment of Cameron Azari as a Notice Specialist. Mr. Azari has over 19 years of experience in the design and implementation of legal notification and claims administration programs, having been personally involved in well over one hundred successful notice programs. Declaration of Cameron R. Azari ("Azari Decl.") on Settlement Notice Plan at ¶¶ 5–7 and Attachment 1.

As set forth below, and in the Notice and Claim Form (SA, Exhibits B, C, and E), the process for submitting a claim is straightforward and the manner in which Settlement Funds will be allocated is simple and efficient, and both treat all members of the Proposed Class fairly and equally. Proposed Settlement Class Members can fill out and mail back a tear-off postcard with postage prepaid, fill out a claim online and submit it electronically using an electronic signature, download a form from the Settlement website, or request a paper copy of a claim form from the Settlement Administrator. In sum, the Court should find that the proposed methods for providing

notice to the Class, including by direct mail, email, and a settlement website, comport with both Rule 23 and due process considerations. Azari Decl. at ¶¶ 28–31.

VIII. Scheduling a Final Approval Hearing Is Appropriate.

The last step in the settlement approval process is a final approval hearing at which the Court may hear all evidence and argument necessary to make its settlement evaluation. Proponents of the proposed Settlement may explain the terms and conditions of the proposed Settlement Agreement, and offer argument in support of final approval. Proposed Settlement Class Members who object to the proposed Settlement may appear and be heard. The Court will determine after the final approval hearing whether the proposed Settlement should be approved, and whether to enter a final order and judgment under Rule 23(e). Plaintiffs request that the Court set a date for a hearing on final approval at the Court's convenience, but no earlier than 120 days after entry of the Preliminary Approval Order, and schedule further proceedings pursuant to the schedule set forth below:

ACTION	DATE
Preliminary Approval Order Entered	At the Court's Discretion
Publication Notice Published	Within 30 days following entry of Preliminary Approval Order
Mailing of Notice Commenced	Within 45 days following entry of Preliminary Approval Order
Notice Date	60 days following the Commencement of Publication Notice
Proof of Notice Submitted	Within 60 days following Notice Date

Exclusion/Objection Deadline	Within 90 days after Notice Date
Final Approval Brief and Response to Objections Due	At least 10 days prior to the Final Approval Hearing
Final Approval Hearing	No earlier than 120 days following the Notice Date
Final Approval Order Entered	At the Court's Discretion
Deadline to Submit Claims	150 days after Notice Date

IX. Conclusion.

For the foregoing reasons, Plaintiff respectfully asks that the Court (1) certify the proposed Settlement Class for settlement purposes only; (2) appoint Elizabeth Black, Catherine Bushman, Krishnendu Chakraborty, Maduhchanda Chakraborty, Ralph Christopherson, Anne Emerson, William Fitch, Eric Forsetter, Mary Fuerst, Debbie Hansen-Bosse, Stuart Hirsch, Ilene Hirsh, Howard Kaplowitz, Barbara Lynch, and Kevin Smith as Settlement Class Representative Plaintiffs; (3) appoint Plaintiffs' Counsel as Class Counsel; (4) grant preliminary approval of the proposed Settlement Agreement; (5) approve the form and manner of notice described above; and (6) grant such further relief the Court deems reasonable and just. For convenience, proposed dates and deadlines leading to a final approval hearing are provided in the proposed order separately submitted to the Court.

DATED: May 30, 2019

TOUSLEY BRAIN STEPHENS PLLC

/s/ Kim D. Stephens

Kim D. Stephens, OSB No. 030635
Jason T. Dennett, *admitted pro hac vice*
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
Email: kstephens@tousley.com
jdennett@tousley.com

Interim Lead Plaintiffs' Counsel

STOLL BERNE

/s/ Keith S. Dubanevich

Keith S. Dubanevich, OSB No. 975200
Yoona Park, OSB No. 077095
209 SW Oak Street, Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840
Email: kdubanevich@stollberne.com
ypark@stollberne.com

Interim Liaison Plaintiffs' Counsel

Tina Wolfson
AHDoot AND WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069
Tel: (310) 474-9111
Fax: (310) 474-8585
Email: twolfson@ahdootwolfson.com

James Pizzirusso
HAUSFELD LLP
1700 K. Street NW, Suite 650
Washington, DC 20006
Tel: (202) 540-7200
Fax: (202) 540-7201
Email: jpizzirusso@hausfeldllp.com

Karen Hanson Riebel
Kate M. Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
Email: khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Plaintiffs' Executive Leadership Committee